# EGY BINOM KONGRUENCIÁRÓL

*DR. KISS PÉTER*

*(Közlésre érkezett: 1977. január 30.)*

## *Bevezetés*

Tekintsük az

$$x^k - x \equiv 0 \pmod{B^n} \tag{1}$$

kongruenciát, ahol $k \geqslant 2$, $B > 1$ és $n$ természetes számok. Ennek megoldása azonos a következő probléma megoldásával: Melyek azok az $x$ egész számok a $B$ alapú számrendszerben, melyekre $x^k$ és $x$ ugyanarra az $n$ jegyű számra végződik?

Ehhez hasonló problémával, különösen a tízes számrendszerben már igen sokat foglalkoztak. (Lásd [4], 453–464. oldal.) Erre utalnak a különböző elnevezések is. G. Valentin [5] szerint már a görög szofisták is észrevették, hogy 5, 25 és 6 számok négyzetei is ugyanezekre a számokra végződnek és ők ezeket ciklikus számoknak nevezték. De más elnevezések is ismertek. Például R. L. Goodstein [6] $n$ indexű automorfikus számoknak nevezte a $B$ alapú rendszerben az $x^2 = x \pmod{B^n}$ kongruencia megoldásait, A. Cunningham [3] pedig (1) megoldásait $n$-edrendű $k$-adfokú kellemes számoknak nevezte a $B$ alapú rendszerben.

A problémát először 1814-ben az Annales de Math. ([1], 220. oldal) fogalmazta meg: „Melyik az a szám, melynek egymásután következő hatványai ugyanarra az $n$ jegyű számra végződnek mint az eredeti szám? Itt elegendő az $x^2 \equiv x \pmod{10^n}$ kongruenciával foglalkozni, mert könnyen belátható, hogy ennek megoldásai kielégítik az $x^k \equiv x \pmod{10^n}$ kongruenciát is minden $k > 2$ természetes szám esetén. Ugyanis, ha $x^2 \equiv x \pmod{10^n}$, akkor $x^k = x^{k-2} \cdot x^2 \equiv x^{k-2} \cdot x = x^{k-1} \equiv \ldots \equiv x \pmod{10^n}$.

A sok eredmény közül, melyek hasonló problémákra vonatkoznak, néhány a következő.

Az Annales de Math. problémáját először M. Tédenat ([1], 309–321. oldal) oldotta meg.

Bebizonyította, hogy az

$$x^2 \equiv x \pmod{10^n} \tag{2}$$

kongruenciának, eltekintve a 00 . . . 0 és a 00 . . . 01 triviális megoldásoktól, minden $n$ esetén két különböző $x_1$ és $x_2$ $n$ jegyű megoldása van. Az egyik 5-re, a másik pedig 6-ra végződik és $x_1 + x_2 = 10^n + 1$. Megadott egy eljárást is, hogyan képezhető az $n = m+1$ esetben a megoldás, ha az $n = m$ eset megoldása ismert.

R. L. Goodstein [6] az

$$x^2 - x \equiv 0 \pmod{B^n} \tag{3}$$

kongruenciával foglalkozott. Bizonyította, hogy ha $B = u \cdot v$ (ahol $(u, v) = 1$) és $uq \equiv 1 \pmod{v}$, akkor az $uq \cdot v^{n-1}$ számot $B^n$-nel osztva, a maradék (3) megoldása (a $B$ alapú számrendszerben $n$ jegyű megoldás, vagy más szóval $B$ alapú $n$ indexű automorfikus szám).

[8]-ban Tédenat eljárásához hasonló rekurziós eljárást adtam a (3) kongruencia megoldására és rámutattam egy kapcsolatra az automorfikus számok és pszeudoprím számok között.

N. P. Callas [11] igazolta, hogy ha $x$ a (2)-nek egy megoldása, akkor

$$y = x^t \sum_{k=0}^{t-1} (-1)^k \binom{t+k-1}{k} \binom{2t-1}{t+k} x^k$$

kielégíti az $y^2 \equiv y \pmod{10^{tn}}$ kongruenciát.

C. P. Popovici [12] az (1) kongruencia megoldásait adta meg explicit alakban $B = 10$ esetben.

Érdemes még megemlíteni, hogy (3) megoldásait számítógéppel is többen keresték. Például Vernon de Guerre és R. A. Fairbairn [14] 1000 (ezer!) jegyre kiszámították az automorfikus számokat 6, 10 és 12 alap esetén, vagyis (3) megoldásait $n = 1000$ és $B = 6$, 10, 12 esetében.

Jelen dolgozatban az (1) kongruencia általános megoldásával foglalkozunk, megadjuk a megoldások számát és a megoldások explicit alakját. Bebizonyítjuk, hogy a tételünkből következményként adódik E. Hewitt egy tétele. Megmutatjuk a tételünknek a pszeudoprím számokkal való kapcsolatát, új bizonyítást adunk R. D. Carmichael egy tételére és megoldjuk K. Szymiczek egy problémáját.

*Egy segédtétel bizonyítása*

Mielőtt rátérünk az (1) kongruencia megoldására, egy segédtételt bizonyítunk.

*1. Tétel:* Legyen $M = q_1 \cdot q_2 \ldots q_r$ egy természetes szám, ahol $q_1 > 1$ és $(q_i, q_j) = 1$ minden $i \neq j$ esetén, továbbá legyen

$$Q_s = \frac{M}{q_s} = q_1 \cdot q_2 \ldots q_{s-1} \cdot q_{s+1} \ldots q_r.$$

Ekkor

$$\sum_{s=1}^{r} Q_s^{\varphi(q_s^k)} \equiv 1 \pmod{M^k},$$

ahol $\varphi$ az Euler-féle függvény.

*Bizonyítás:* A feltételek miatt elég bizonyítani, hogy $\sum_{s=1}^{r} Q_s^{\varphi(q_s^k)} - 1$ osztható $q_i^k$-val minden $i = 1, 2, \ldots, r$ esetén. A

$$\sum_{s=1}^{r} Q_s^{\varphi(q_s^k)} - 1 = \sum_{s=1}^{i-1} Q_s^{\varphi(q_s^k)} + \sum_{s=i+1}^{r} Q_s^{\varphi(q_s^k)} + Q_i^{\varphi(q_i^k)} - 1$$

kifejezés első két összegének minden tagja osztható $Q_s$ definíciója miatt $q_i$ valamely $\varphi(q_i^k)$ hatványával, ezért $q_i^k$-val is. Ugyanis könnyen belátható, hogy $q_j \geqslant 2$ esetén $\varphi(q_j^k) \geqslant k \cdot$ $\cdot Q_j^{\varphi(q_j^k)} - 1$ pedig Euler kongruencia tétele miatt osztható $q_i^k$-val, mert $Q_i$ és $q_i^k$ relatív prímek. Ezzel igazoltuk az 1. Tételt.

*Az általános eset megoldása*

Most rátérünk az $x^k - x \equiv 0 (\text{mod } B^n)$ kongruencia megoldására. Nem megy az általánosság rovására, ha feltesszük, hogy $n = 1$, hiszen $B$ lehet teljes $n$-edik hatvány is. Legyen $B$ alakja $B = 2^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_r^{\alpha_r}$, ahol $2 = p_1, p_2, \ldots, p_r$ különböző prímek.

Vezessük be a következő jelöléseket. Legyen $i > 1$ esetén $g_i$ primitív gyök (mod $p_i^{\alpha_i}$), $d_i = (k-1, \varphi(p_i^{\alpha_i}))$, $k-1 = d_i \cdot d_i'$ és $\varphi(p_i^{\alpha_i}) = d_i \cdot c_i$; ha pedig $i = 1$, akkor $g_1 = 5$ továbbá ha $\alpha_1 < 2$, akkor $c' = c_1' = 1$ és ha $\alpha_1 \geqslant 2$ akkor $c' = 2, c_1' = 2^{\alpha_1 - 2}$, azonkívül $d = (k-1, c'), d_1 = (k-1, c_1'), k-1 = d \cdot d' = d_1 \cdot d_1', c' = d \cdot c$ és $c_1' = d_1 \cdot c_1$ ($\varphi$ az Euler-féle függvényt, $[x, y]$ pedig $x$ és $y$ legnagyobb közös osztóját jelöli.)

További jelölések: $P_i = \dfrac{B}{p_i^{\alpha_i}} = p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} \cdot p_{i-1}^{\alpha_i + 1} \ldots p_r^{\alpha_r}$, azonkívül $i > 1$ esetén legyen $G_i = 0$ vagy $G_i = g_i^{c_i \cdot q_i}$; $i = 1$ esetén pedig ha $\alpha_1 = 0$, akkor $G_1 = 0$ és ha $\alpha_1 > 0$, akkor $G_1 = 0$ vagy $G_1 = (-1)^{c' \cdot q} \cdot g_1^{c_1 \cdot q_1}$, ahol $q = 0, 1, \ldots, d-1$ és $q_i = 0, 1, \ldots, d_i - 1$.

Ezen jelöléseket felhasználva, a következő tételt fogjuk bizonyítani.

*2. Tétel:* Az

$$x^k - x \equiv 0 \ (\text{mod } B) \tag{4}$$

kongruencia összes megoldása

$$x \equiv \sum_{i=1}^{r} G_i \cdot P_i^{\varphi(p_i^{\alpha_i})} \ (\text{mod } B).$$

*Bizonyítás:* (4) ekvivalens az

$$\begin{aligned} &x^k - x \equiv 0 \ (\text{mod } 2^{\alpha_1}) \\ &x^k - x \equiv 0 \ (\text{mod } p_2^{\alpha_2}) \\ &\cdot \\ &\cdot \\ &\cdot \\ &x^k - x \equiv 0 \ (\text{mod } p_r^{\alpha_r}) \end{aligned} \tag{5}$$

kongruenciarendszerrel. Oldjuk meg először az

$$x^k - x \equiv 0 \ (\text{mod } p_i^{\alpha_i}) \tag{6}$$

kongruenciát, ahol $i > 1$, így $p_i > 2$ prímszám.

$x$ és $x^{k-1} - 1$ relatív prímek, ezért (6)-ból

$$x \equiv 0 \ (\text{mod } p_i^{\alpha_i})$$

vagy $x^{k-1} \equiv 1 (\text{mod } p_i^{\alpha_i})$. (7)

(7)-ben $x$ alakja a $g_i$ primitív gyök segítségével

$$x \equiv g_i^{\beta_i} \ (\text{mod } p_i^{\alpha_i})$$

ahol $0 \leqslant \beta_i < \varphi(p_i^{\alpha_i})$. Ezt (7)-be írva

$$g_i^{(k-1)\beta_i} \equiv 1 \equiv g_i^0 \ (\text{mod } p_i^{\alpha_i}),$$

amiből

$$(k-1)\beta_i \equiv 0 \ \left(\text{mod } \varphi(p_i^{\alpha_i})\right). \tag{8}$$

Ebből következik, hogy $(k-1)\beta_i = d_i \cdot d_i' \cdot \beta_i$ osztható $\varphi(p_i^{\alpha_i}) = d_i \cdot c_i$-vel, amiből $(d_i', c_i) = 1$ miatt $c_i$ osztója $\beta_i$-nek, vagyis $\beta_i = c_i \cdot q_i$. Itt $\beta_i$ határai miatt $0 \leqslant q_i < d_i$.
Tehát (6) megoldásai:

$$x \equiv 0, \quad x \equiv g_i^{c_i q_i} (\mathrm{mod}\ p_i^{\alpha_i})$$

melyek száma ($q_i$ lehetséges értékei miatt) $d_i+1$ és különböznek egymástól (mod $p_i^{\alpha_i}$).

Az

$$x^k - x \equiv 0 \ (\mathrm{mod}\ 2^{\alpha_1}) \tag{9}$$

kongruenciát (6)-hoz hasonló módon oldhatjuk meg.

Itt ha $\alpha_1 > 0$, akkor

$$x \equiv 0 \ (\mathrm{mod}\ 2^{\alpha_1})$$

vagy $x^{k-1} \equiv 1 (\mathrm{mod}\ 2^{\alpha_1})$ (10)

De (10)-ben $(x, 2^{\alpha_1}) = 1$, ezért mint ismeretes $x$ alakja

$$x \equiv (-1)^{\beta} \cdot g_1^{\beta_1} (\mathrm{mod}\ 2^{\alpha_1}),$$

ahol $0 \leqslant \beta < c'$, $0 \leqslant \beta_1 < c_1'$ és $g_1 = 5$. Ezt (10)-be írva

$$(-1)^{(k-1)\beta} \cdot g_1^{(k-1)\beta_1} \equiv 1 \equiv (-1)^0 \cdot g_1^0 (\mathrm{mod}\ 2^{\alpha_1}),$$

amiből

$$(k-1) \cdot \beta \equiv 0 \ (\mathrm{mod}\ c')$$

$$(k-1) \cdot \beta_1 \equiv 0 \ (\mathrm{mod}\ c_1').$$

Innen az előzőekhez hasonlóan $\beta = c \cdot q$ illetve $\beta_1 = c_1 \cdot q_1$ adódik, ahol $0 \leqslant q < d$ és $0 \leqslant q_1 < d_1$.
Tehát (9) megoldásai $\alpha_1 > 0$ esetén

$$x \equiv 0, \ x \equiv (-1)^{c \cdot q} \cdot g_1^{c_1 q_1} (\mathrm{mod}\ 2^{\alpha_1})$$

melyek száma $d \cdot d_1 + 1$ és különböznek egymástól (mod $2^{\alpha_1}$).

Ha $\alpha_1 = 0$, akkor az egyetlen megoldás nyilván $x \equiv 0 \ (\mathrm{mod}\ 1)$.

Az (5) kongruenciarendszer minden kongruenciája felbontható tehát lineáris kongruenciákra és így

$$\begin{aligned} x &\equiv G_1 (\mathrm{mod}\ 2^{\alpha_1}) \\ x &\equiv G_2 (\mathrm{mod}\ p_2^{\alpha_2}) \\ &\cdot \\ &\cdot \\ &\cdot \\ x &\equiv G_r (\mathrm{mod}\ p_r^{\alpha_r}) \end{aligned} \tag{11}$$

alakra hozható, ahol $G_1 = 0$ ha $\alpha_1 = 0$ és $G_1 = 0$ vagy $G_1 = (-1)^{c \cdot q} \cdot g_1^{c_1 \cdot q_1}$ ha $\alpha_1 \neq 0$, továbbá $G_i = g_i^{c_i \cdot q_i}$ vagy $G_i = 0$ ha $i > 1$. $G_i$ lehetséges értékeit figyelembe véve (11) nyilván $(d \cdot d_1 + 1)(d_2+1) \ldots (d_r+1)$ illetve $\alpha_1 = 0$ esetén $(d_2+1) \ldots (d_r+1)$ kongruenciarendszert ad, melyek (mod $B$) különböző megoldásokat szolgáltatnak.

Szorozzuk meg (11) $i$-edik sorát $P_i^{\varphi(p_i^{\alpha_i})}$-vel $\left(P_i = \frac{B}{p_i^{\alpha_i}}\right)$, ekkor a modulus $\varphi(p_i^{\alpha_i}) \geqslant 1$

és $P_i$ definíciója miatt osztható $B$-vel. Ezért

$$P_i^{\varphi(p_i^{\alpha i})} \cdot x \equiv P_i^{\varphi(p_i^{\alpha i})} \cdot G_i \pmod{B}.$$

Elvégezve a szorzásokat $i = 1, 2, \ldots, r$ esetben és a kapott kongruenciákat összeadva kapjuk:

$$x \cdot \sum_{i=1}^{r} P_i^{\varphi(p_i^{\alpha i})} \equiv \sum_{i=1}^{r} G_i \cdot P_i^{\varphi(p_i^{\alpha i})} \pmod{B}.$$

De az 1. Tétel miatt $x$ együtthatója kongruens 1-gyel mod $B$, ezért

$$x \equiv \sum_{i=1}^{r} G_i \cdot P_i^{\varphi(p_i^{\alpha i})} \pmod{B},$$

amit bizonyítani akartunk.

*Egy példa*

A 2. Tétel alkalmazásaként oldjuk meg az

$$x^3 - x \equiv 0 \pmod{10^2} \tag{12}$$

kongruenciát.

Jelen esetben $k = 3, B = 10^2, p_1 = 2,\ p_2 = 5,\ , g_2 = 2$ (mert 2 primitív gyök (mod $5^e$) minden $e$ természetes szám esetén), $c' = 2, c_1' = 2^0 = 1, d = (k-1, c') = 2, d_1 = (k-1, c_1') = 1, c = \frac{c'}{d} = 1, c_1 = \frac{c_1'}{d_1} = 1, d_2 = (k-1, \varphi(5^2)) = 2, c_2 = \frac{\varphi(5^2)}{d_2} = 10,$

$P_1 = 5^2$ és $P_2 = 2^2$.

A 2. Tétel alapján (12) megoldásai

$x \equiv G_1 \cdot 5^{\varphi(2^2)} + G_2 \cdot 2^{\varphi(5^2)} = G_1 \cdot 5^2 + G_2 \cdot 2^{20} \pmod{10^2}$ alakúak, ahol $G_1 = 0$ vagy $G_1 = (-1)^q \cdot 5^{q_1}$ $(q = 0,1; q_1 = 0)$ és $G_2 = 0$ vagy $G_2 = 2^{10 q_2}$ $(q_2 = 0,1)$.
Tehát $G_1 \cdot 5^2 = 0, 25, -25 \equiv 0, 25, 75$ és $G_2 \cdot 2^{20} = 0, 2^{20}, 2^{30} = 0, 76, 24 \pmod{10^2}$ és így a megoldások

$$x_1 \equiv 0 + 0 \equiv 0$$
$$x_2 \equiv 0 + 76 \equiv 76$$
$$x_3 \equiv 0 + 24 \equiv 24$$
$$x_4 \equiv 25 + 0 \equiv 25$$
$$x_5 \equiv 25 + 76 \equiv 1$$
$$x_6 \equiv 25 + 24 \equiv 49$$
$$x_7 \equiv 75 + 0 \equiv 75$$
$$x_8 \equiv 75 + 76 \equiv 51$$
$$x_9 \equiv 75 + 24 \equiv 99 \pmod{10^2}.$$

Az eredményből az is következik, hogy azok a számok a tízes számrendszerben, melyek harmadik hatványai ugyanarra a kétjegyű számra végződnek, mint az eredeti szám, azok, melyek 00, 01, 24, 25, 49, 51, 75, 76 vagy 99 végződésűek.

A kapott eredmény megegyezik N. I. Nedita [10]-beli eredményével.

*Következmények*

I. A 2. Tételből következik, hogy (4) kongruenciának annyi különböző megoldása van (mod $B$), ahányféleképpen meg tudjuk választani a $G_1, G_2, \ldots G_r$ értékeket, vagyis: Az $x^k - x \equiv 0 \pmod{B}$ kongruencia megoldásainak száma

$$M = D \cdot (d_2+1) \cdot (d_3+1) \ldots (d_r+1),$$

ahol $D = 1$ ha $\alpha_1 = 0$ és $D = d \cdot d_1 + 1$ ha $\alpha_1 \neq 0$. A többi paraméter jelentése ugyanaz, mint a 2. Tételben.

II. A 2. Tételből következik, hogy (4) megoldásai, $k$ értékeit változtatva, csak $d$ és $d_i$ értékektől függenek. De ha $(k_1-1, \varphi(B)) = (k_2-1, \varphi(B))$, akkor a megfelelő $d$ és $d_i$ értékek egyenlőek, így igaz a következő tétel:

*3. Tétel:* Ha $(k_1-1, \varphi(B)) = (k_2-1, \varphi(B))$, akkor

$$x^{k_1} - x \equiv 0 \pmod{B}$$

$$x^{k_2} - x \equiv 0 \pmod{B}$$

kongruenciák ekvivalensek.

Speciális esetként adódik, hogy $x^2 - x \equiv 0 \pmod{B}$ megoldásai szolgáltatják az $x^k - x \equiv 0 \pmod{B}$ összes megoldását, ha $k-1$ és $\varphi(B)$ relatív prímek.

III. $B = 10$ esetén $g_2 = 2$ minden $n$-re. Ezeket a 2. Tételbe helyettesítve és felhasználva az 1. Tételből következő $2^{\varphi(5^n)} - 1 \equiv -5^{\varphi(2^n)} \pmod{10^n}$ összefüggést, C. P. Popovici [12]-ben bizonyított tételét kapjuk speciális esetként.

IV. E. Hewitt [7] bizonyította, hogy akkor és csak akkor létezik olyan $k$ természetes szám, melyre

$$x^k - x \equiv 0 \pmod{B}$$

azonosan teljesül, ha $B$ négyzetmentes. Ez a 2. Tételből is következik. A kongruencia azonosan csak akkor teljesül, ha a megoldásainak $M$ számára $M = B$. De az előzőek alapján

$$M = D \cdot (d_2+1) \ldots (d_r+1) \leqslant \prod_{i=1}^{r} (\varphi(p_i^{\alpha_i})+1) \leqslant \prod_{i=1}^{r} p_i^{\alpha_i} = B$$

és az egyenlőség akkor és csak akkor áll fenn mindenhol, ha $\alpha_i = 1$ és $(p_i-1) \mid (k-1)$ minden $i = 1, 2, \ldots, r$ esetén, ezért valóban igaz E. Hewitt tétele. Bizonyításunkból az is következik, hogy $k$ akkor és csak akkor elégíti ki a feltételeket, ha többszöröse a $(p_i-1)$ egész számok legkisebb közös többszörösének.

*A pszeudoprím számokról*

Az $n$ természetes számot pszeudoprím számnak nevezzük az $a$ egész szám vonatkozásában, ha $n$ összetett és

$$a^n \equiv a \pmod{n}, \tag{13}$$

továbbá abszolút pszeudoprímnek nevezzük, ha $n$ minden $a$ természetes szám vonatkozásában pszeudoprím.

Könnyű belátni, hogy minden összetett $n$ természetes szám végtelen sok $a$ egész vonatkozásában pszeudoprím, még akkor is ha megkívánjuk, hogy $n$ és $a$ relatív prímek legyenek. Ugyanis tetszőleges összetett $n$ esetén, ha $a = n \cdot k+1$ (ahol $k$ tetszőleges egész), akkor $(n, a) = 1$ és nyilván (13) is teljesül, ezért $n$ pszeudoprím az $a$ vonatkozásában.

K. Szymiczek a következő kérdést tette fel: Melyek azok az $n$ összetett természetes számok, melyek csak az $a = n \cdot k+1$ alakú egészek vonatkozásában pszeudoprímek az $(n, a) = 1$ feltétel mellett? (Lásd A. Rotkiewicz [13], 143. oldal, Problem, 46). A következőkben választ adunk K. Szymiczek kérdésére, bebizonyítjuk a következő tételt.

*4. Tétel:* Egy $n$ összetett természetes szám $(n, a) = 1$ feltétel mellett akkor és csak akkor csupán az $a = n \cdot k+1$ alakú egészek vonatkozásában pszeudoprím, ha $(n-1, \varphi(n)) = 1$. (A tételt más megfogalmazásban lásd [9]-ben).

*Bizonyítás:* Legyen $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

A 2. Tétel bizonyításából következik, hogy az

$$x^n \equiv x \pmod{n}$$

kongruencia $n$-hez relatív prím megoldásainak száma akkor és csak akkor 1, ha $d = d_1 = d_2 = \ldots d_r = 1$, vagyis ha $(n-1, \varphi(p_i^{\alpha_i})) = 1$ minden $i = 1, 2, \ldots, r$ esetén. Ez a feltétel azonban ekvivalens az $(n-1, \varphi(n)) = 1$ feltétellel és az egyetlen $(x, n) = 1$ feltételt kielégítő megoldás nyilván $x \equiv 1 \pmod{n}$ vagyis $x = k \cdot n+1$. Ebből, és az $a$ vonatkozású pszeudoprímek definíciójából már következik az állítás.

Megjegyezzük, hogy végtelen sok olyan $n$ természetes szám létezik, mely kielégíti a 4. Tétel feltételeit. Ilyenek például az $n = 2^k$ vagy az $n = 2p$ ($p$ prím) alakú számok, hiszen $(2^k-1, 2^{k-1}) = 1$ és $(2p-1, p-1) = 1$.

Vizsgáljuk most meg, hogy mi a feltétele annak, hogy egy összetett $n$ természetes szám abszolút pszeudoprím legyen. A definíció alapján $n$ nyilván akkor és csak akkor abszolút pszeudoprím, ha a (13) kongruencia indentikusan teljesül. Ennek feltételét viszont már megadtuk az előzőekben, E Hewitt tételének bizonyítása során: $n$ négyzetmentes, és ha $n = p_1, p_2, \ldots p_r$, akkor $(p_i-1) \mid (n-1)$ minden $i = 1, 2, \ldots, r$ esetén. A feltételekből az is következik, hogy $n$ páratlan ($p_1 \neq 2$), mert ellenkező esetben $n-1$ páratlan és így nem osztható egy páros $p_i-1$ egész számmal. De az is következik, hogy $r \geqslant 3$, ugyanis $r = 2$ esetén $(p_1-1) \mid (p_1p_2-1)$ relációból $p_1p_2-1 = (p_1-1)p_2+p_2-1$ miatt $(p_1-1) \mid (p_2-1)$ és hasonlóan $(p_2-1) \mid (p_1-1)$ adódna, amiből $p_1 = p_2$ következne. Ez viszont lehetetlen, mert már láttuk, hogy $n$ négyzetmentes.

Tehát a következő eredményt kaptuk:

*5. tétel:* Egy $n$ összetett természetes szám akkor és csak akkor abszolút pszeudoprim, ha páratlan, négyzetmentes, legalább három különböző páratlan prímtényező szorzata és $n$ minden $p$ prímtényezőjére $(p-1) \mid (n-1)$.

Ezt a tételt először R. D. Carmichael [2] bizonyította, a mi bizonyításunk azonban különbözik az általa adott bizonyítástól.

*IRODALOM*

[1] Annales de Math., 5 (1814–15).
[2] R. D. Carmichael, Note on a new number theory funcion, Bull of the Amer. Math. Soc., 16 (1910), 232–238.
[3] A. Cunningham: On agreeable numbers, British Assoc. Report, 1893, 699.
[4] L. E. Dickson, History of the theory of numbers, Chelsea Publ. Co., New York, 1971, vol. I.
[5] Forhandlinger i videnskabs-selsk. i Christiania, 1901 (Oversigt over Selsk. Moder; 1901), 3–13.
[6] R. L. Goodstein, Numbers in a general scale, Math. Gaz., 43 (1959), 270–272.
[7] E. Hewitt, Certain congruences that hold identically, Amer. Math. Monthly, 83 (1976), 270–271.
[8] P. Kiss, On one way of making automorphic numbers, Publ. Math. Debrecen, 22 (1975), 199–203.
[9] P. Kiss, Aufabe 768, Elemente der Math., 31 (1976), 72.
[10] N. I. Nedita, O problema de teoria numerelos, Gazeta Matematica, ser. A, 73 (1968), 191–196.
[11] Nicholas P. Callas, Representations of automorphic numbers, Fibonacci Quart., 10 (1972), 393–396, 402.
[12] C. P. Popovici, Une généralisation d'une equation arithmétique de D. Pompeiu, Bull. Math. de la Soc. Sci. Math. de Roumania, Tome 13 (61), 1969, 73–84.
[13] A. Rotkiewicz, Pseudoprime numbers and their generalizations, University of Novi Sad, 1972.
[14] Vernon de Guerre and R. A. Fairbairn, Automorphic numbers, Journal of Recr. Math., Vol. 1 (1968), 173-179.

## ON A BINOM CONGRUENCE

*BY PÉTER KISS*

In this paper we solve a generalization of a classical problem. The problem was drawn first up in the Annales de Math. ([1], p. 220): What is the number of which successive powers end in the same number of $n$ digits as the originál number? This problem leads to the solution of the congruence $x^2-x \equiv 0 \pmod{10^n}$. We solve the congruence $x^k-x \equiv 0 \pmod{B^n}$, where $k$, $B$ and $n$ are fixed integers, and we give the explicit form of the solutions and the number of solutions.

We show that some results of N. I. Nedita [10], C. P. Popivici [12], E. Hewitt [7] and R. D. Carmichael [2] follow from our results. We solve a problem of K. Szymiczek (see [13], problem 46, p. 143) concerning pseudoprime numbers, as an application of our results.